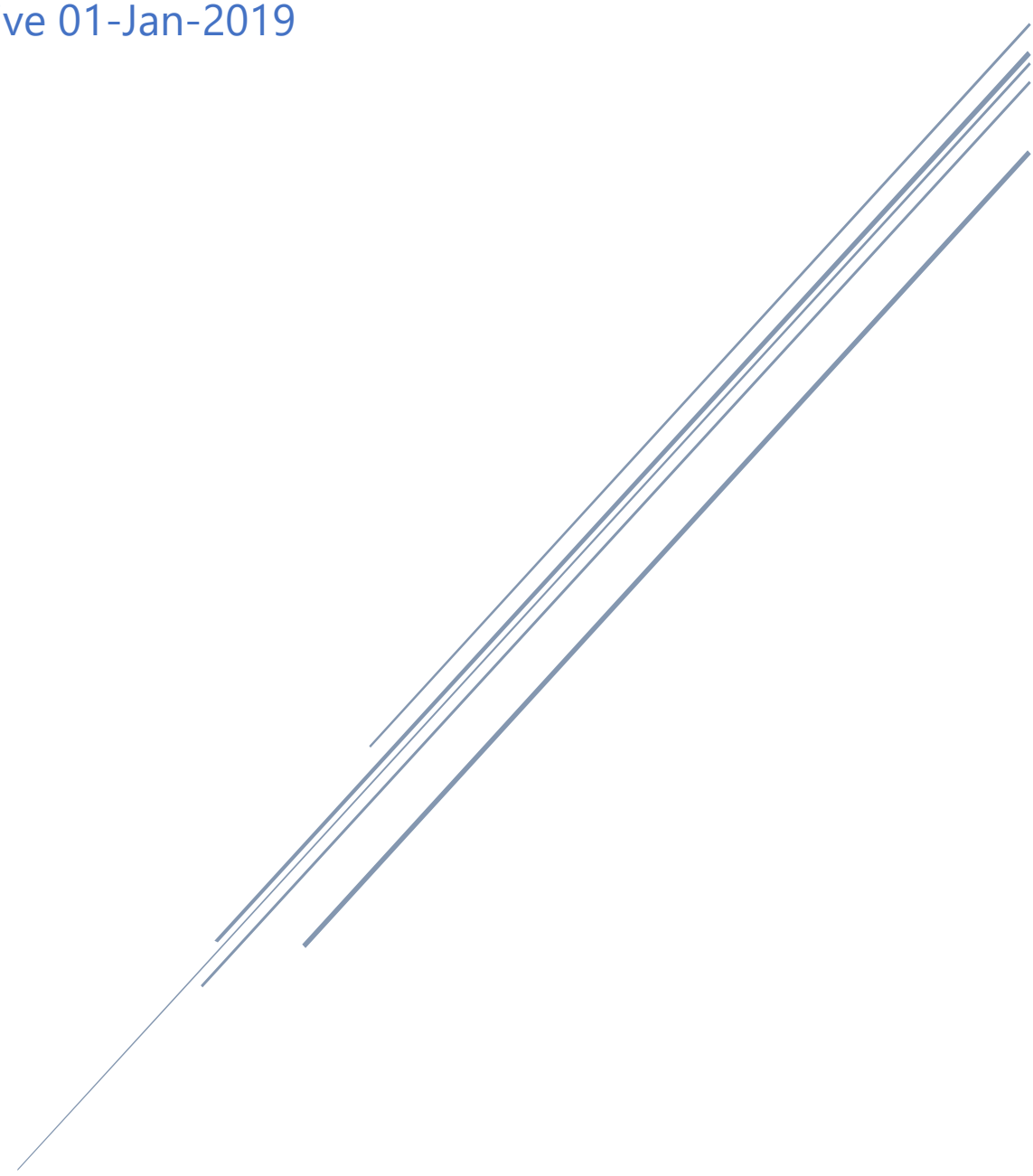
Mandai Park Holdings Information Security Policy (External Party)

Version 1.7

Effective 01-Jan-2019



Content Page

1 Definitions

In this document, the following words and expressions have the following meanings set out hereunder:

Application Business Owner	refers to the business stakeholder that owns the IT application
Application IT Manager	refers to the IT lead that is in charge of the support for the IT application
"Company Electronic Data"	refers to all electronic data and/or information, not limited to data / information related to/about WRS's employees, transactions, customers, financial, tenders, plans, partners, vendors, patents, formulas or new technologies that is created / acquired / processed / distributed / used / stored / owned by WRS Group & its employees
"Company IT Assets"	Systems, Application/Software, Data, Services (including but not limited to cloud services), Hardware, Equipment (including but not limited to Computing Devices, docking station, display monitor, keyboards, mouse, presentation pointers, cables, physical storage media, Computing Devices) owned and/or operated/used/consumed by MPH Group.
"Company IT Infrastructure"	Datacentre, Servers, Network and its equipment owned and/or operated/used/consumed by MPH Group.
"Company IT Network"	refer to Company IT Assets that are in the internal network and not served openly over the Internet without the use of VPN.
"Company"	refers to MPH, MPD, WRS and their subsidiaries
"Computing Devices"	refers to any devices that has computing capabilities including but not limited to desktops, laptops, tablets, smartphones, smart TVs and IoTs
"Network-enabled Devices"	refers to any devices that can have network connectivity, including Computing Devices, routers, access points, switches, hub, etc
"DPO"	means Data Protection Officer, and refers to the appointee in Legal
"Employee"	refers to any person(s) employed by MPH, MPD, WRS, SZG, JBP and WRSCF.
"External Party"	refers to any parties, individual or company (e.g. vendors, supplier, auditors, partners) that is not within the Company
"HOD"	means Head of Department and/or Team Lead.
"IT Helpdesk"	refers to the helpdesk support email (it.helpdesk@wrs.com.sg) for WRS IT
"JBP"	means The Jurong Bird Park Private Limited.
"Misuse / Misconduct"	refer to but not limited to, Unauthorized use, wrong or improper use, embezzlement, fraud.
"MPD"	means Mandai Park Development Pte Ltd.
"MPH"	means Mandai Park Holdings; also refers to WRS and MPD as a group.
"NS"	means Night Safari park.
"PC"	means Personal Computers and refers to laptops, desktops, tablets that runs on Windows and Macintosh operation systems
"Policy"	refers to this document, IT Policy, Standards and Guidelines
"RS"	means River Safari park.
"SOP"	means Standard Operating Procedure.
"SZG"	means Singapore Zoological Gardens.
"VPN"	Virtual Private Network
"WRS ExCo"	refers to the WRS Executive Committee (not limited to, namely the Chiefs)
"WRS Finance"	means WRS Finance department.
"WRS IT"	means WRS Information Technology department.
"Legal"	means Legal department.
"WRS Procurement"	means WRS Procurement department.
"WRS"	means Wildlife Reserves Singapore and refers to WRS, SZG, NS, RS, JBP as a group

All other terms will be reference from SANS, see https://www.sans.org/security-resources/glossary-of-terms/

2 Introduction

2.1 Purpose

2.1.1 This document (aka This Policy), part of a group of MPH IT Policies, provides the framework for the management of Company IT Infrastructure, Assets and Data.

2.1.2 **MPH Information Security Policy for External Party** defines the requirements and conduct which External Party shall comply, to protect the confidentiality, integrity, availability, and authenticity of Company IT Assets & Data. This policy applies to all External Party unless otherwise stated. All External Party must read, understand, agree and comply to.

2.2 Responsibility, Authority and Distribution

2.2.1 WRS IT holds the responsibility and authority to define, review and maintain this Policy.

2.2.2 This Policy shall be reviewed by WRS IT HOD and updated as per necessary.

2.2.3 WRS IT will seek WRS ExCo approvals for this Policy annually.

2.2.4 This Policy shall be published by WRS IT and made available to all Employees over Intranet; and made available to External Parties via their official email.

2.3 Inquiry, Addition / Exception and Escalation

2.3.1 Inquiries regarding this Policy shall be directed to WRS IT (#IT-Governance <it.gov@wrs.com.sg>).

2.3.2 Department can layer on additional policies to meet their specific business needs on the condition that additions are aligned with this Policy. Department to seek WRS IT guidance when creating additional policies.

2.3.3 Exception requests to this Policy to be requested to WRS IT. Exception shall be reviewed and approved by WRS IT HOD on a case by case basis.

2.3.4 Escalation to be directed to the Chief Financial Officer.

2.4 Disciplinary / Recourse

2.4.1 Cases of misuse / misconduct related to the WRS IT Policies, Standards and Guidelines may lead to disciplinary and/or legal action(s) by the Company.

3 Information Security for External Party

3.1 Conduct

3.1.1 External Party is responsible for taking reasonable care of Company IT Assets, not limited to Computing Devices, docking station, display monitor, keyboards, mouse, presentation pointers, cables, physical storage media issued to and put under his/her care; This includes keeping them under lock and key.

3.1.2 In the event of misused, damaged and/or lost due to negligence, the cost of replacement shall be solely borne by the External Party.

3.1.3 Company proprietary information stored on Computing Devices whether owned or leased by Company, the employee or a third party, remains the sole property of the Company.

3.1.4 External Party has a responsibility to promptly report theft, loss or unauthorized disclosure of WRS proprietary information to WRS IT.

3.1.5 External Party has a responsibility to promptly report any misconduct, ill intent and cybersecurity events to WRS IT; Cybersecurity events include, but are not limited to:

- Scanning of Company IT Asset and Networks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

3.1.6 External Party who identify, label, handle, or dispose of Company IT assets shall comply with the requirements according to its data classifications as defined by Legal.

3.1.7 Company IT Assets provided by the Company are provided exclusively for the conduct of the Company's business in accordance to section 4.1 Acceptable Usage Policy (AUP).

3.1.8 External Party shall abide by access control rules layout in this Policy, regardless if the access control rules are automated through authentication settings or communicated by this Policy.

3.1.9 External Party who handle Company Data shall comply to the data classifications and usage policy defined by Legal.

3.1.10 External Party who handle information on Company's behalf shall protect it to keep it confidential, as appropriate, and use it only for valid business purposes.

3.1.11 Company email account should be used for Company-related purposes.

3.1.12 External Party is prohibited from using USB devices on Point-of-Sales (POS) Computing Devices / terminals / machines.

3.1.13 External Party is prohibited from using Point-of-Sales (POS) Computing Devices / terminals / machines to access unauthorised sites.

3.1.14 External Party shall not circumvent any security software and measures.

3.2 Computing, Software, Peripherals and related Devices

3.2.1 External Party shall be issued Company IT Assets on their Application Business Owner or project manager's request.

3.2.2 External Party shall ensure Computing Devices under his/her care are either switched off or protected with screensaver lock when he/she is not present within visible range of their computing device.

3.2.3 External Party shall ensure that Computing Devices are up-to-date as such it is their responsibility switch off / reboot their Computing Devices daily, to allow the updates of Computing Device's OS, software, configuration and anti-virus definitions.

3.2.4 External Party is recommended to switch the Bluetooth settings to use the hidden mode (non-discoverable); and only activate Bluetooth only when it is needed.

3.2.5 External Party shall not install or use software that are not approved by WRS IT. Please refer to Authorised Applications Standards.

3.2.6 External Party is recommended to use WRS IT issued Storage Media (e.g. USB / Thumbdrive, Memory stick, External Harddisk) when performing their role and responsibilities.

3.2.7 External Party shall ensure that the Computing Devices that they use to access our network, asset & data have up-to-date patches, and anti-virus software with up-to-date definitions installed on the device. Anti-virus end-point protection need to be in the Gartner's Magic Quadrant for End-Point protection.

3.3 System User Identity

3.3.1 External Party's System User Identity shall be created by WRS IT upon the request from Application Business Owner or project manager and approvals from respective Application IT Manager.

3.3.2 External Party to use his/her unique System User Identity issued/endorsed by WRS IT when accessing Company IT Network and Company IT Assets to perform his/her roles and responsibilities.

3.4 Password Protection

3.4.1 External Party is prohibited from sharing personal password information and other authentication methods with anyone.

3.4.2 External Party shall ensure passwords conform to the standards defined in section 4.2 Password Construction Standards.

3.4.3 External Party shall not use the same password for Company accounts as for other non-Company access (for example, personal ISP account, option trading, benefits, and so on); and where possible, shall not use the same password for multiple account/access.

3.4.4 External Party must protect his/her password and **shall not**:

- Have passwords inserted into email messages, Alliance cases or other forms of electronic communication.
- Reveal passwords over the phone to anyone.
- Reveal passwords on questionnaires or security forms.
- Hint at the format of a password (for example, "my family name").
- Share passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Write passwords down and store them anywhere in your office or store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Use the "Remember Password" feature of applications (for example, web browsers).

3.4.5 Any External Party suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.5 Network Access Rights

3.5.1 External Party **must only use** WRS IT approved Network-enabled Devices to access Company IT Network; Personal Computing Devices are prohibited from accessing Company IT Network that are not accessible directly over the Internet.

3.5.2 External Party cannot bring and plug in personal Network-enabled Devices to Company IT Network without WRS IT approval.

3.5.3 WRS IT reserves the right to review External Party's Cybersecurity Policy if necessary.

3.5.4 External Party shall ensure that their Computing Devices are adequately protected against virus and keyloggers when using their personal Computing Devices to access Company IT Assets that is available over Internet, not limited to Company Web Services (e.g. Administration) and Cloud Services (like Email / Intranet);

3.5.5 External Party is strongly discouraged to connect their Computing Devices to unsecured Wi-fi (e.g. Public Wi-Fi hotspots) where login and password information may be compromised. External Party is strongly encouraged, where need to connect, connect thru Telco ISP. Please see section 4.3 Connect Securely Best Practices for reference.

3.6 Business System Access Rights

3.6.1 External Party is authorized to only access information systems based on their job functions and responsibilities with request and justification from Application Business Owner or project manager and subjected to the approval of Application IT Manager.

3.6.2 Application Business Owner or project manager shall exercise discretion, based on "least rights" and "need to know" principles when requesting for their External Party's access and privilege to.

3.7 Email / Electronic Documents / Collaboration Tools

3.7.1 External Party shall not use Company email for non-work-related correspondence.

3.7.2 Official electronic documents shall be stored in the Intranet or Department Sites, or other storage media provided by WRS IT.

3.7.3 Document owners/creators are required to label Company Data according to the appropriate classification standards.

3.7.4 External Party are responsible for the protection and management of documents entrusted to them and should adhere to the standards and guidelines defined in the Workplace Collaboration Standards and Guidelines and protected according to its data classifications as defined by Legal.

3.7.5 External Party shall not to circumvent the labels, or any mechanisms put in place for Data Privacy and Loss Prevention.

3.7.6 External Party must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3.8 File Transfer with External Systems

3.8.1 External Party will be provided with a Secured File Transfer Protocol (SFTP) account for file exchanges with the organisation on a need-to basis with request and justification from Application Business Owner or project manager subjected to the approvals from respective Application IT Manager.

3.9 Server Access Rights

3.9.1 External Party to submit a system deployment plan and approved by respective Application IT Manager.

3.9.2 External Party shall install a remote access software for remote access to Company IT Infrastructure. Please refer to Approved Remote Access Methods.

3.9.3 External Party shall be provided with remote access for remoting into Company IT Infrastructure on a need-to basis with request from Application Business Owner or project manager and approvals from WRS IT Infra Lead.

3.9.4 External Party shall only access from static IP(s). External Party shall provide proof of ownership of the static IP(s) that will be accessing Company IT Asset to WRS IT for whitelisting.

3.9.5 External Party access shall be restricted by time period, IPs, services (ports/protocols) and monitored.

3.9.6 While using a Company-owned computer to remotely connect Company corporate network, External Party shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

3.10 Disable User Identity

3.10.1 The Company reserves the right to suspend/disable External Party's System User Identity should there be any misuse/breach of IT systems. Disablement of External Party's User Identity shall be requested by Application Business Owner or project manager.

3.10.2 All systems access and privileges associated to External Party shall be disabled, unless instructed by the request.

3.11 Termination of engagement with External Party

3.11.1 Exiting External Party shall perform clearance with WRS IT, and must ensure:

- all Company IT Assets are returned, in its entirety.
- all access rights are removed.

3.12 Logging and Monitoring

3.12.1 Company is not obliged to, but may monitor activities and communications without prior notice.

4 Appendixes

4.1 Acceptable Usage Policy (AUP)

4.1.1 Individuals **shall not**:

- Use the Internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which the Company considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the Internet or email to make personal gains or conduct a personal business.
- Use the Internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Use automatic forwarding of Company email to a third-party email system; Individual messages which are forwarded by the user must not contain Company confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Company business, to create or memorialize any binding transactions, or to store or retain email on behalf of the Company. Such communications and transactions should be conducted through proper channels using Company-approved documentation.
- Send unprotected sensitive or confidential information externally.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the Internet without prior approval of WRS IT.
- Make fraudulent offers of products, items, or services originating from any Company account.
- Make statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effect security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the External Party is not an intended recipient or logging into a server or account that the he/she is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods,

packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to WRS IT is made.
- Executing any form of network monitoring or interception of data unless this activity is a part of the External Party's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Company IT Network.
- Interfering with or denying service to any user other than the External Party's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Company Employees to parties outside without proper authorisation.
- Unauthorized use, or forging, of email header information.

4.2 Password Construction Standards

4.2.1 All passwords should meet or exceed the following characteristics

- Contain at least 8 alphanumeric characters.
- Contain both upper-case and lower-case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

4.2.2 All passwords **shall not** have the following characteristics

- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

4.2.3 You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)

4.2.4 A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

4.3 Connect Securely Best Practices

4.3.1 When connecting Company's notebook to any network, please take note of the type of network, and the risks/mitigation

4.3.2 Examples of trusted network

- Office
- Home (Please refer to paragraph 4.3.5)
- Usage of USB Modem or WIFI via Telco network

4.3.3 Examples of Un-trusted network

- Hotel LAN
- Hotel WIFI
- Airport WIFI
- Public WIFI/Hotspot (Eg. Café)
- Third-party LAN or WIFI

4.3.4 Risks/Mitigation based on scenarios

Connections	Via Trusted Network	Via Un-trusted Network	Type of risk mitigated
Send/receive emails via the email server	No issue as email communication to/from the email server is encrypted	1. No issue as email communication to/from the email server is encrypted 2. Alternatively connect using personal USB modem or WIFI via 3G Phones to download emails	1. This will prevent unauthorized personnel from sniffing your email contents

		3. Encrypt when sending confidential emails	
Accessing Internal applications	No issue	1. Not encouraged to access internal applications directly unless absolutely necessary. 2. Establish VPN session before accessing internal applications 3. Alternatively connect using personal USB modem or WIFI via 3G Phones to access	1. When VPN session is established, all traffic to the Company is encrypted 2. This will prevent unauthorized personnel from sniffing your surfing contents
Normal surfing	Beware of unknown sites	Beware of unknown sites	NOTE: Make sure your anti-virus and software patches are kept up to date.

4.3.5 All home wireless infrastructure devices that provide access to Company IT Assets should adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password